ELECTRONIC WARFARE FOR CYBER WARRIORS

GRADUATE RESEARCH REPORT

Daniel E. Rauch, Major, USAF

AFIT/ICW/ENG/08-10

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/ICW/ENG/08-10

ELECTRONIC WARFARE FOR CYBER WARRIORS

GRADUATE RESEARCH REPORT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of in Cyber Warfare

Daniel E. Rauch, BS

Major, USAF

June 2008

AFIT/ICW/ENG/08-10

ELECTRONIC WARFARE FOR CYBER WARRIORS

Daniel E. Rauch, BS

Major, USAF

Approved:

/// SIGNED /// _____

Robert F. Mills, PhD (Member) Date

/// SIGNED /// _____

Timothy H. Lacey, MS (Member) Date

Abstract

This research paper provides complete course content for the AFIT EENG 509, Electronic Warfare class. It is intended as a replacement for the existing course and designed for Intermediate Developmental Education (IDE) students in the Cyber Warfare degree program. This course provides relevant academic courseware and study material to give cyber warriors an academic and operational perspective on electronic warfare and its integration in the cyber domain.

Table of Contents

page

page

AFIT/ENG/08J

ELECTRONIC WARFARE FOR CYBER WARRIORS

I. Introduction

Background

In May 2007, twelve Intermediate Developmental Education (IDE) students entered the Air Force Institute of Technology's (AFIT) Cyber Warfare degree program. Eleven military and one civilian embarked upon a 12 month journey to become cyber warriors and leaders in this new domain. They are the future leaders in cyberspace operations. Unfortunately, the inability in the Air Force and Department of Defense (DoD) to agree upon roles and responsibilities, or even a common definition of cyberspace, has led the Cyber Warfare program down an ill-paved path. AFIT, an academic institution, lacks the operational experience and expertise to provide a "warfare" program that meets the needs of its IDE graduate students.

These students are future military leaders and require increased breadth of knowledge in cyberspace capabilities and vulnerabilities, not in-depth technical knowledge. Trying to provide a small group of individuals a relevant education in a relatively new field of study is problematic. Providing appropriate, but more importantly relevant, content is a struggle for an inexperienced AFIT staff.

While most of AFIT's instructors are PhDs, they lack operational experience in cyber warfare. This is no slight to their individual capabilities as the world is still struggling to define the cyber domain. Course content for a cyber warfare degree includes computer network attack and defense, computer forensics, electronic warfare, and the obligatory technical math courses. Although instructors at AFIT are

knowledgeable in the above fields, there are few who have operational experience, and can relate their subjects to war fighting. This problem lends itself to the development of overly-technical courses providing little insight for our warrior leaders. Unlike systems engineering, or logistics, cyber warfare requires an operational flavor that AFIT (or any academic institution) is unlikely to have.

This paper attempts, in part, to rectify this problem. Both by bringing to light the problem and by providing an example of appropriate course content, I hope to steer future course development in the right direction.

Motivation

The United States military's primary purpose is to hold at risk for death and destruction the individuals, organizations, and nation states that jeopardize our national security. As such, relevant military education, especially when lauding "warfare" in the title, should embrace that purpose. After several months of cyber warfare education, I realized that AFIT does not have the experience, resources, or energy to create relevant course content for all classes. In particular, the Electronic Warfare course, EENG 509, completely lacked an operational flavor. EENG 509 is the emphasis of this paper.

Purpose

This paper provides a new course outline, content, reading material, and mid-term and final exams for the EENG 509 Electronic Warfare course. The purpose is to improve the quality and focus of education for our cyber warriors.

Scope

The intent of the new EENG 509 course is to meet the following objectives:

1) Understand the fundamental principles of Electronic Warfare (EW).
2) Understand the basics of radar and infrared theory.
3) Gain a competent understanding of current threat systems.
4) Gain a competent understanding of current CAF capabilities and tactics.
5) Gain a working understanding of the relationship between EW and the cyber domain.

Upon completion of this course, students should have a conversational level of expertise in EW and be able to confidently relate the principles of EW to the cyber domain. This course is not designed to make students electronic warfare officers, but to give them the broad conceptual understanding needed to ask the right questions and make good decisions during acquisition and operational planning.

Assumptions

The information provided assumes this course will be taught to IDE cyber warfare students by an AFIT instructor with an electrical engineering background. The paper also assumes the course will be taught at the SECRET level.

Overview

While the bulk of the information for EENG 509 is contained in the appendices of this document, the following chapters provide references, outline the course, and provide additional sources of information for future use. Chapter two provides a brief overview of

the sources used in deriving the EENG 509 course content. Chapter 3 outlines the course and describes the individual lessons. Chapter 4 concludes with additional subject areas and references to update course material.

II. Reference Validation

The bulk of the courseware for EENG 509 was derived from the USAF Weapons Instructor Course (WIC) academics. These academics are unique in that they are taught to students with a wide variety of backgrounds and areas of expertise (e.g. an F-15E Pilot with a BS in electrical engineering and an Intel Officer with a BA in history). The WIC courseware is continually reviewed and updated for every incoming class. The academics are only available to graduates of the Weapons Instructor Course and are not meant to be widely disseminated in their complete form. Where WIC academics were used in the EENG 509 courseware, the material was thoroughly reviewed to tailor the content to the IDE audience and remove excessive operation jargon.

Additional references and briefings were used as needed to meet the course objectives or provide additional perspective. The non-exhaustive list of references in the bibliography is repeated in each appendix as applicable. Each lesson has references sourced in that lesson. Certain classified references only appear in the associated classified appendix.

III. Course Outline

Overview

The majority of material for this course is contained in the Appendices. Other than Appendices A, O, and AC, all are classified. Below is a brief discussion of each lesson. These appendices are not for public release. Dissemination is controlled by AFIT/ENG.

Syllabus

Appendix A contains the syllabus which highlights the course layout and objectives.

Introduction

Appendix B contains slides and notes for the first lesson**.** The introduction section, as well as handling the administrative portion of the course, is an overview briefing on the fundamentals of EW. The lesson covers common terminology and highlights the similarities and differences of information operations, electronic warfare, and cyber warfare.

Appendix C contains reading on Operation Overlord recommended prior to this lesson. This brief highlights discussion information operations during Operation Overlord and the impact on WWII.

History of EW

Appendix D contains lesson 2, History of EW. This lesson starts with the invention of the telegraph and following technological developments over a 200 year period, showing the military application of technology and the impact on warfare.

Blue Voice Communication

Appendix D contains lesson 3, Blue Voice Communication. The emphasis of this lesson is modern radio communication to include secure radio and Have Quick radios. The lesson discusses the capabilities and limitations as well as the potential threat against our current systems.

Appendix F contains a recommended reading on the Global IO Threat.

Data Links

Appendix G contains the slides for lesson 4, Data Links. This lesson discusses the evolution of our modern tactical data links, the terminology, integration, and the capabilities and limitations. The goal of the lesson is to provide a working knowledge of current systems and introduce the student to near-term follow-on systems.

History of Modern Radar

Lesson5, History of Modern Radar is contained in Appendix H. This lesson is the most technical with emphasis on radar theory. The goal is to provide a foundation for the implications of the capabilities and limitations highlighted in later lessons.

Modern Radar Threats

Appendix I contains lesson 6, Modern Radar Threats. This lesson discusses, from acquisition to impact, the modern radar surface-to-air missile threat.

Appendix J contains recommended reading discussing China's assessed capabilities and limitations. This reading applies to the rest of the course.

IR Theory

Appendix K contains lesson 7, IR Theory. This lesson is similar in structure to the History of Modern Radar lesson and walks the student through the EO portion of the electro-magnetic spectrum.

Modern IR Threats

Appendix L, lesson 8, Modern IR Threats, covers the plethora of infrared guided surface-to-air missile systems. Capabilities, limitations, and proliferation are discussed.

IR Counter Measures

Appendix M contains lesson 9, IR Counter Measures. This lesson, while briefly discussing radar countermeasures and expendables, emphasizes infrared countermeasures. The discussion contains systems designed for military and commercial aviation.

Red Air Threat

Appendix N contains lesson 10, Red Air Threat. The emphasis for this lesson is the proliferation and availability of 4^{th} generation aircraft and upgrades to counter the US military's current dominant posture.

NASIC Tour

The course instructor will be responsible for setting up a tour and briefings at NASIC to cover material applicable to this course.

Mid Term Exam

Appendix O contains an outline for the course midterm. This test is an essay-style take-home exam designed to test synthesis application of the course material

covered in lesson 1 through 10. The emphasis is not on electrical engineering principles, but on concepts that can be applied to operational and acquisition decision making. The recommended timeline for this exam is one week.

Air Defense Systems / Integrated Air Defense Systems

Appendix P contains lesson 11, Air Defense Systems (ADS) and Integrated Air Defense Systems (IADS). This lesson starts with the factors that define an air defense system and make that system "integrated". The lesson brings in the concept of the kill chain and highlights the structured and hierarchical approach most countries take with their IADS.

Appendix Q contains a recommended reading. The Electronic Warfare Integration Guide covers planning considerations and integrated EW employment.

RCA Lab Tour

This tour shall be set up by the course instructor.

Jammers

Appendices R contains lesson 12, Jammers. Designed to emphasize the capabilities of current red air jamming systems, this lesson highlights the combat Air Forces's current interest. Appendix S contains a recommended supplementary brief on additional jamming systems.

Suppression of Enemy Air Defenses

Appendix T contains lesson 13, Suppression of Enemy Air Defenses (SEAD). This lesson discusses current capabilities and limitations of CAF SEAD and DEAD (destruction of enemy air defenses) platforms. The lesson emphasizes the methods used to disrupt the kill chain of an IADS.

Appendix U contains the After Action Report from the Electronic Warfare Coordination Cell Operation Iraqi Freedom.

Low Observables

Appendix V contains the slides for lesson 14, Low Observables (LO). This lesson discusses LO theory and basic principles as well as operational considerations and the effect on the kill chain.

EW and Modern Networks

Appendices W, X, Y, Z, AA contain individual briefings for lesson 15. These briefs discuss the current vulnerabilities and threat to modern networks.

Appendix AB contains ACC EW Concept of Operations document, a recommended reading.

Final

Appendix AC contains an outline for the EENG 509 final exam. Similar in structure to the midterm, this is comprehensive final designed to demonstrate knowledge appropriate to meeting the course objectives. Recommended timeline for this final is 10 days.

IV. Conclusion/Future Expansion

This research project provides adequate course material for the AFIT IDE EENG 509, Electronic Warfare class. This class will serve as an invaluable part of the Cyber Warfare syllabus and provide graduates with the conceptual knowledge needed in their future careers.

References for Updates

Certain aspects of this course (in particular lessons 12 and 15) may quickly become dated material. Links are provided in those presentations to update the course material when available.

Additional Subject Areas

Given appropriate security clearance and facilities, additional relevant course content may be available. I recommend contacting the 563 FTS at Randolph (DSN 487-9364) for additional information.

Bibliography

1. Joint Publication 3-13. 2006. *Information Operations*. Joint Electronic Library. http://www.dtic.mil/doctrine/jpoperationsseriespubs.htm
2. Joint Publication 3-13.1. 2007. *Electronic Warfare*. Joint Electronic Library. http://www.dtic.mil/doctrine/jpoperationsseriespubs.htm
3. DoD Dictionary. http://www.dtic.mil/doctrine/jel/doddict/index.html
4. The National Military Strategy for Cyberspace Operations. 2006. http://www.maxwell.af.mil/au/awc/awcgate/awc-doct.htm#nms
5. USAF Weapons Instructor Course Academics AVS510A, *Integrated Air Defense Systems*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx
6. Bellis, M. *The History of the Electric Telegraph and Telegraphy*. Retrieved 30 Apr 2008 from http://inventors.about.com/od/tstartinventions/a/telegraph.htm
7. Bellis, M. *The History of the Telephone*. Retrieved 30 Apr 2008 from http://inventors.about.com/od/bstartinventions/a/telephone.htm
8. CivilWarTraveler. *Virginia Valley & Mountains*. Retrieved 30 Apr 2008 from http://www.civilwartraveler.com/EAST/VA/va-valley/morevalley.html
9. Wikipedia. History of the Radio. Retrieved 30 Apr 2008 from http://en.wikipedia.org/wiki/History_of_radio
10. Lerner, A. 2006. *Spanish American War*. Encyclopedia of Espionage, Intelligence, and Security. Retrieved 30 Apr 2008 from http://findarticles.com/p/articles/mi_gx5211/is_2004/ai_n19126694

11. Wikipedia. *History of the Radar*. Retrieved 1May 2008 from http://en.wikipedia.org/wiki/History_of_radar
12. Wikipedia. *AIM-9 Sidewinder*. Retrieved 2 May 2008 from http://en.wikipedia.org/wiki/AIM-9_Sidewinder
13. Wikipedia. *AGM-45 Shrike*. Retrieved 1 May 2008 from http://en.wikipedia.org/wiki/AGM-45_Shrike
14. Wikipedia. *Wild Weasel*. Retrieved 1 May 2008 from http://en.wikipedia.org/wiki/Wild_Weasel
15. Warner, W. 2004. *Great Moments in Microprocessor History*. Retrieved 1May 2008 from http://www.ibm.com/developerworks/library/pa-microhist.html
16. Wikipedia. *History of the Internet*. Retrieved 2 May 2008 from http://en.wikipedia.org/wiki/History_of_the_Internet
17. Jane's. 2002. *EL/L-8222 self-protection jamming pod (Israel), AIRBORNE ELECTRONIC WARFARE (EW) SYSTEMS*. Retrieved 1 May 2008 from http://www.janes.com/extracts/extract/jav/jav_9059.html
18. USAF Weapons Instructor Course Academics AVS540P, *F-15E Have Quick Radio Capabilities and Limitations*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx
19. USAF Weapons Instructor Course Academics AVS542I, *C-17A Secure Radio Principles*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx
20. USAF Weapons Instructor Course Academics CCC155A, *Introduction to Tactical Data Links*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx

21. USAF Weapons Instructor Course Academics AVS659N, *F-15C Fighter Data Link.* http://www.nellis.af.smil.mil/acad/acad/curr.aspx
22. USAF Weapons Instructor Course Academics EMP363P, *F-15E Air-to-air Fighter Data Link Employment.* http://www.nellis.af.smil.mil/acad/acad/curr.aspx
23. USAF Weapons Instructor Course Academics PPP420P, *Introduction to Radar and Pulse-Doppler Principles*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx
24. Stimson, G. 1983. *Introduction to airborne radar*. Hughes Aircraft Co.
25. AFTTP 3-1.2. *MISSION EMPLOYMENT TACTICS, TACTICAL THREAT REFERENCE GUIDE AND COUNTERTACTICS.*
26. USAF Weapons Instructor Course Academics CWX450A, *Threat Radar Surface-to-Air Missiles Capabilities and Limitations*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx
27. USAF Weapons Instructor Course Academics PPP206A, *Fundamental and Basic Application of the Infrared Spectrum*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx
28. Saville, M. Lecture Notes. 2007. *Introduction to EW Fundamentals*. EENG509.
29. USAF Weapons Instructor Course Academics CWX460A, *Threat Infrared Surface-to-Air Missiles Capabilities and Limitations.* http://www.nellis.af.smil.mil/acad/acad/curr.aspx
30. USAF Weapons Instructor Course Academics AVS656P, *F-15E ALE-45 Countermeasures Dispensers Capabilities and Limitations*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx

31. Taylor, B. *EO/IR Countermeasures Technology Brief*. AFRL/SNJW. 53rd Wg FMS Briefing. Retrieved 13 May 2008 from http://www.53wg.eglin.af.smil.mil

32. USAF Weapons Instructor Course Academics CWX100A, *Threat Aircraft and Armament – Capabilities and Limitations*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx

33. USAF Weapons Instructor Course Academics CWX101A, *Advanced Threat Aircraft and Armament – Capabilities and Limitations*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx

34. USAF Weapons Instructor Course Academics SSS262N, *AIM-120 AMRAAM Capabilities and Limitations*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx

35. Thirtyacre, D. *USAFWC Emerging Threat Tactics Team (EA)*. Retrieved 14 May 2008 from http://www.nellis.af.smil.mil/units/57ATG/ET3.htm

36. USAF Weapons Instructor Course Academics EMP630A, *Suppression of Enemy Air Defenses (SEAD)*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx

37. AFIWC EW Planning and Integration Guide.

38. USAF Weapons Instructor Course Academics PPP652A, *Introduction to Low Observable Principles*. http://www.nellis.af.smil.mil/acad/acad/curr.aspx

39. Johnson, C. 2007. *Foreign Network Warfare Threats to USAF Airborne Networks*. Retrieved 15 May 2008 from http://www.nellis.af.smil.mil/units/57ATG/ET3/07-3/07-3.htm

40. Briefing. 2007. *Emerging Threats to the SIPRNET*. Retrieved 15 May 2008 from http://www.nellis.af.smil.mil/units/57ATG/ET3/07-3/07-3.htm

41. Trollman, D. *Threats to the GIG: A Front Line Defenders Perspective*. Retrieved 15 May 2008 from http://www.nellis.af.smil.mil/units/57ATG/ET3/07-3/07-3.htm

Vita

Maj Daniel Rauch was born and grew up in Milwaukee, WI. After receiving his baccalaureate in electrical engineering from Embry-Riddle Aeronautical University in Prescott, AZ and getting commissioning through ROTC, he spent 4 years at Edwards AFB, CA as a Flight Test Engineer working on aircraft survivability programs. Maj Rauch attended pilot training in 1998 and went on to become an F-15E pilot. He is a graduate of the USAF Weapons School and has 4 combat tours in Afghanistan and Iraq. He is a senior pilot with over 1700 hours, including over 450 hours in combat. His last assignment prior to attending AFIT was as the Assistant Director of Operations for the 422 Test and Evaluation Squadron, Nellis AFB.

APPENDICES

Appendix A

COURSE DESCRIPTION: This course provides a foundation in Electronic Warfare designed specifically for students in the Cyber Warfare program. A baseline technical knowledge of radar and IR/UV/EO is provided, however, the emphasis of the course is on modern systems and tactics that the CAF faces on today's battlefield.

COURSE OBJECTIVES:

- Understand the fundamental principles of Electronic Warfare
- Understand the basics of radar and infrared theory
- Gain a competent understanding of current threat systems (i.e. be able to hold a reasonable discussion with the CSAF)
- Gain a competent understanding of current CAF capabilities and tactics
- Gain a working understanding of the relationship between EW and the Cyber domain

Lesson Title	Lesson Description	Classification	Time (hours)
Introduction	Class overview and discussion of the parallels between EW and Cyber. Introduction of the concepts of Electronic Attack, Electronic Protection, and Electronic Support.	U	1
History of EW	Starting with the telegraph, this class will provide historic examples of EW.	S	1
Blue Voice Communication	Discussion of modern radio systems (with emphasis on Have Quick and KY-58), and the shortcomings of our current equipment.	S	2
Data Link	Tactical Data Links with emphasis on link 16.	U	2
History of Modern Radar	Electrical engineering 101 with emphasis of transmission and antenna theory.	U	2
Modern Radar Threats	Discussion of Early warning, target tracking and engagement radars, and airborne interceptor radars. The goal is to provide the student a broad base of knowledge on the systems the CAF faces on today's battlefields.	S	2
IR Theory Class	Electrical Engineering 101b with emphasis on the advantages and shortcoming of the IR and UV spectrum for target tracking and identification. Emphasis will be on transmission theory, factors affecting these systems, and design and employment considerations.	S	2
Modern IR Threats	Discussion will focus primarily on target tracking end-game systems from SA-7s to modern IR/EO systems. Emphasis will be on giving the student a broad base of threat and proliferation knowledge.	S	2
IR Countermeasures	Current and upcoming IR/EO countermeasures.	S	1
Red Air Threat	The goal is to provide a baseline of knowledge in red/grey threats and current	S	2

Appendix A

	USAF tactics so that all students have an understanding of the scope of the current red EA issues confronting the CAF.		
NASIC Tour	The emphasis here will be to have a field trip and look at cool stuff.	S	2
MID TERM Exam	Take home exam covering the concepts up to this point.	S	N/A
ADS/IADS	Discussion of Air Defense Systems and Integrated Air Defense Systems. This will bring the last several lessons together. Emphasis will be on how IADS fuse information from using a multi-spectral series of dispersed systems.	S	2
RCA Lab Tour	Tour of the AFRL Virtual Combat Lab Facility	S	2
Jammers	Discussion will include both blue/grey and red jammers. The goal is to introduce the student to the plethora of jamming hardware and software available and the ongoing testing and TTP development to counter the threat.	S	2
SEAD	The goal of this lesson is to introduce the student to the mission of Suppression of Enemy Air Defenses, the equipment we currently use, and the plan for the future. While emphasis will be on SEAD, discussion will include DEAD as well.	S	2
Low Observables	Discussion on the principles and modern uses of LO technology.	U	1
EW and Modern Networks	The goal of this lesson is to get the student to consider the possibilities of modern computer network attack and emphasis will be on Blue vulnerabilities.	S	1
Final Exam	Comprehensive take-home exam	S	N/A

CLASSIFIED

Appendix O

UNCLASSIFIED (SECRET when filled in)

EENG 509 MIDTERM EXAM

INSTRUCTIONS

This is not a math test. Answers should demonstrate a competent understanding of the concepts discussed in class.

SECURITY

Answers to questions 3 and 4 may be classified. To avoid potential security issues, you should answer those questions on a SIPR computer and email them to the instructor (please mark the document appropriately). Answers to questions 1, 2, and 5 may be accomplished and emailed via NIPR.

1) Briefly describe, differentiate between, and give examples of electronic attack, electronic support, and electronic protection.

2) Are MIDS and TADIL-J compatible? Briefly discuss the relationship between the terms.

3) If a ROLAND launches a missile at a Fighting Falcon (small airplane flown by little men in insignificant wars) will the ALR-69 consistently provide the pilot with appropriate reaction time for a "heart of the envelope shot"? Discuss why or why not. (Remember this is not a math test; relate the capabilities of the ROLAND and ALR-69 to your radar theory knowledge).
This link may help:
http://ewtoolbox.eglin.af.smil.mil/doc/systems/alr69/69hb1312.pdf

4) What are the advantages and disadvantages of building a missile launch warning system that solely uses the UV spectrum?

5) In less than 500 words, provide an example of effective electronic warfare planning that had an operational or strategic impact on the campaign.

Appendix AC

CLASSIFIED

Appendix AC

UNCLASSIFIED (SECRET when filled in)

FINAL EXAM

INSTRUCTIONS

This is a comprehensive exam on your knowledge of the concepts discussed throughout the class.

SECURITY

Complete this exam and email to the instructor via SIPR.

1) Briefly describe the differences between and ADS and an IADS. Give a real-world example of each.

2) In your opinion, is the CAF lacking in tactical level EA? In other words, are the enemy's airborne tactical jammers better than ours? Discuss why this may be (even if you disagree).

3) Briefly discuss and give examples of how SEAD and LO can break the enemy's kill chain. Is the cost of building a stealth aircraft justified, or should we put our eggs in another basket?

4) What are the vulnerabilities to our airborne data links and what avenues of attack might our enemies take to exploit or deny us the use of those data links? Consider end-to-end connectivity in your discussion.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
19-06-2008	**Master's Graduate Research Project**	June 2007 - June 2008

4. TITLE AND SUBTITLE

Electronic Warfare for Cyber Warriors

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Maj Daniel Rauch

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
This space intentionally left blank.

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
Appendices are classified SECRET, for dissemination contact AFIT/ENG

14. ABSTRACT

This research paper provides complete course content for the AFIT EENG 509, Electronic Warfare class. It is intended as a replacement for the existing course and designed for Intermediate Developmental Education (IDE) students in the Cyber Warfare degree program. This course provides relevant academic courseware and study material to give cyber warriors an academic and operational perspective on electronic warfare and its integration in the cyber domain.

15. SUBJECT TERMS
Electronic Warfare course description, syllabus and content.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Robert F. Mills, PhD (ENG)
U	**U**	**U**	**UU**	30	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6076; e-mail: robert.mills@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18